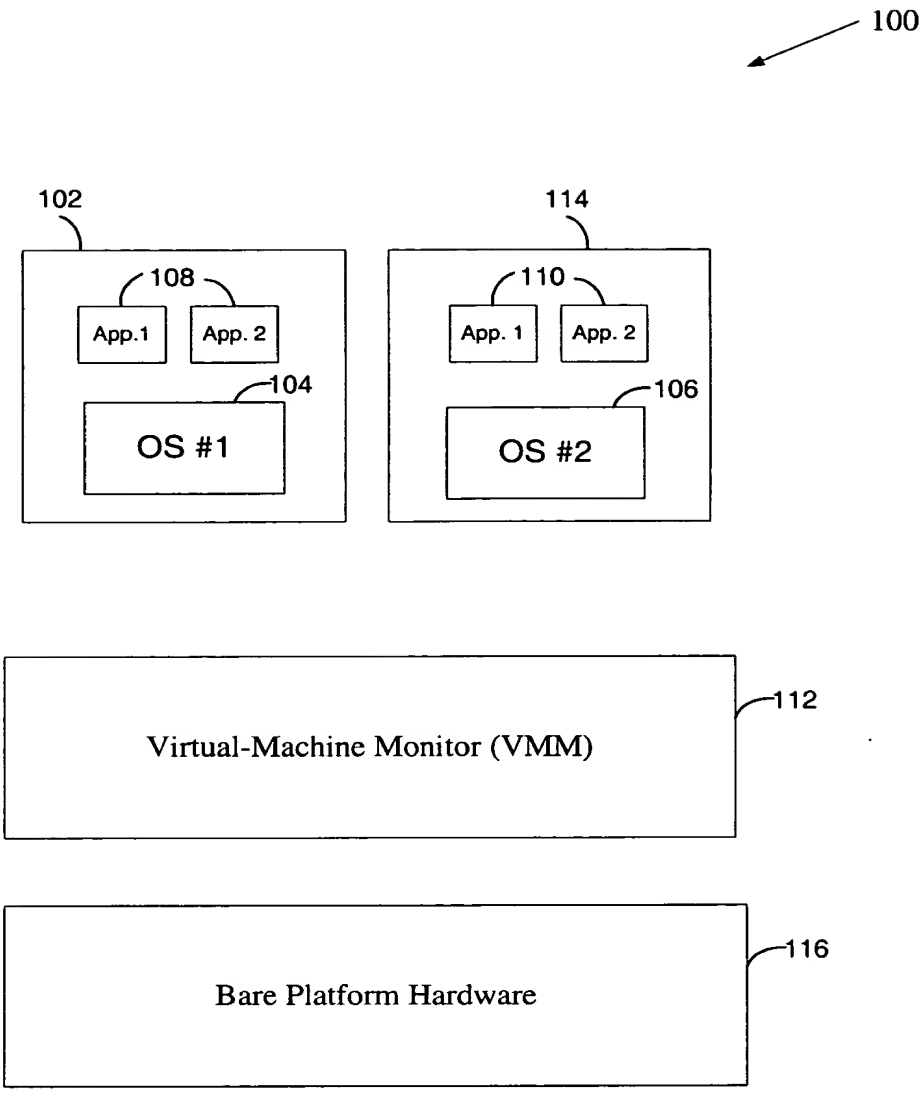
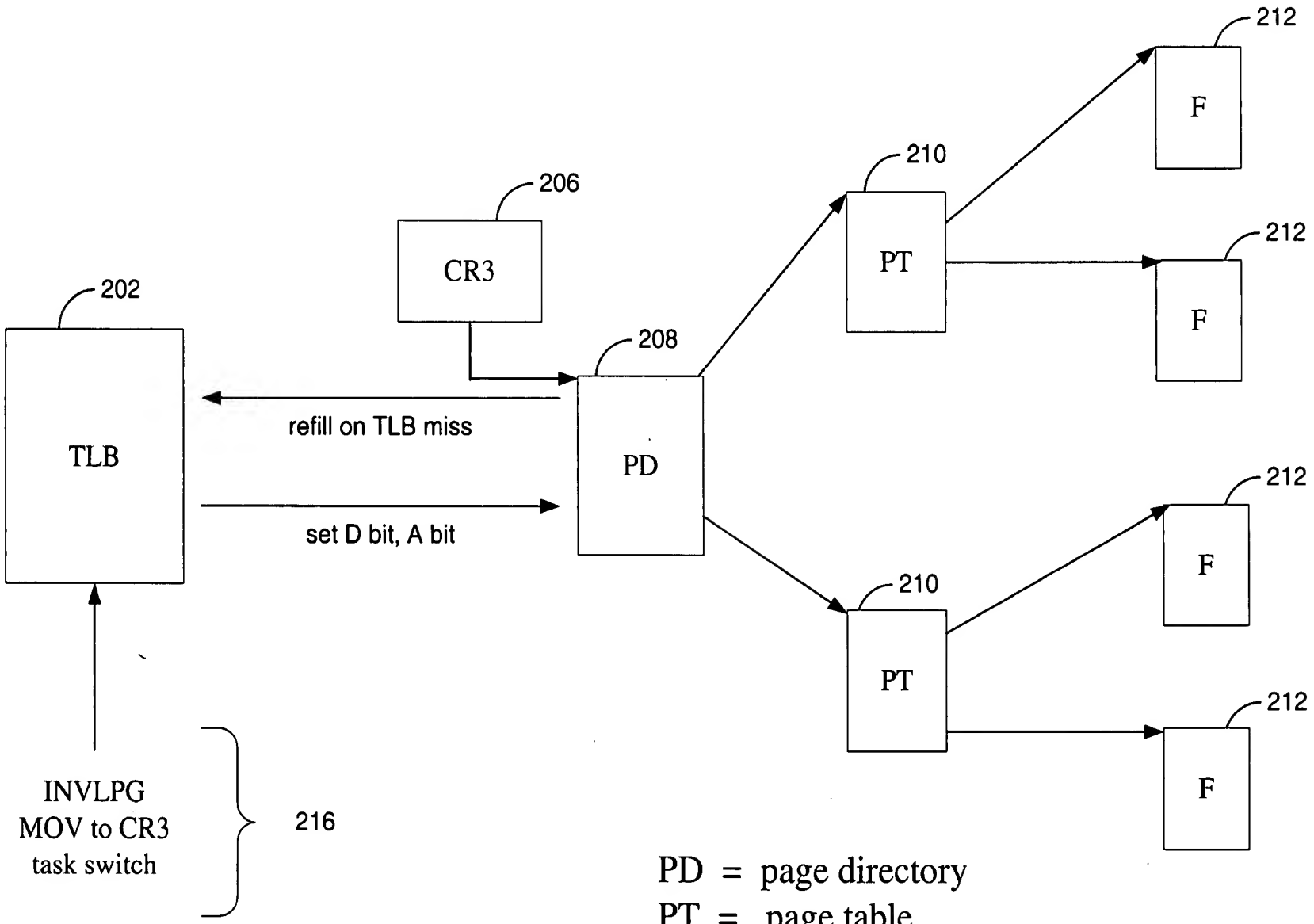
DOCKET: 5050-0



Prior Art

FIG. 1

00722T"EET25760



Prior Art

FIG. 2

00721T "EET25760

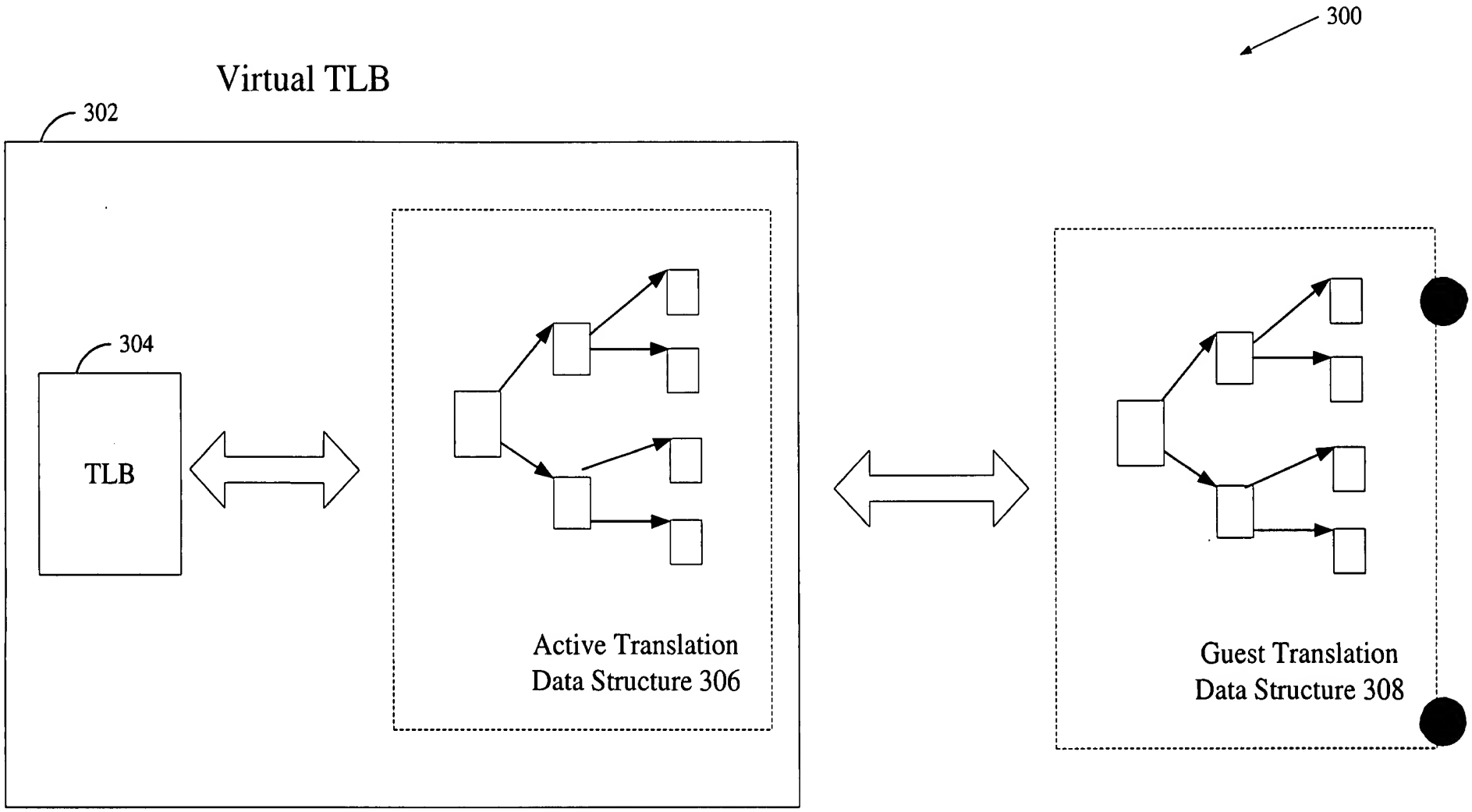


FIG. 3

0605.P14350

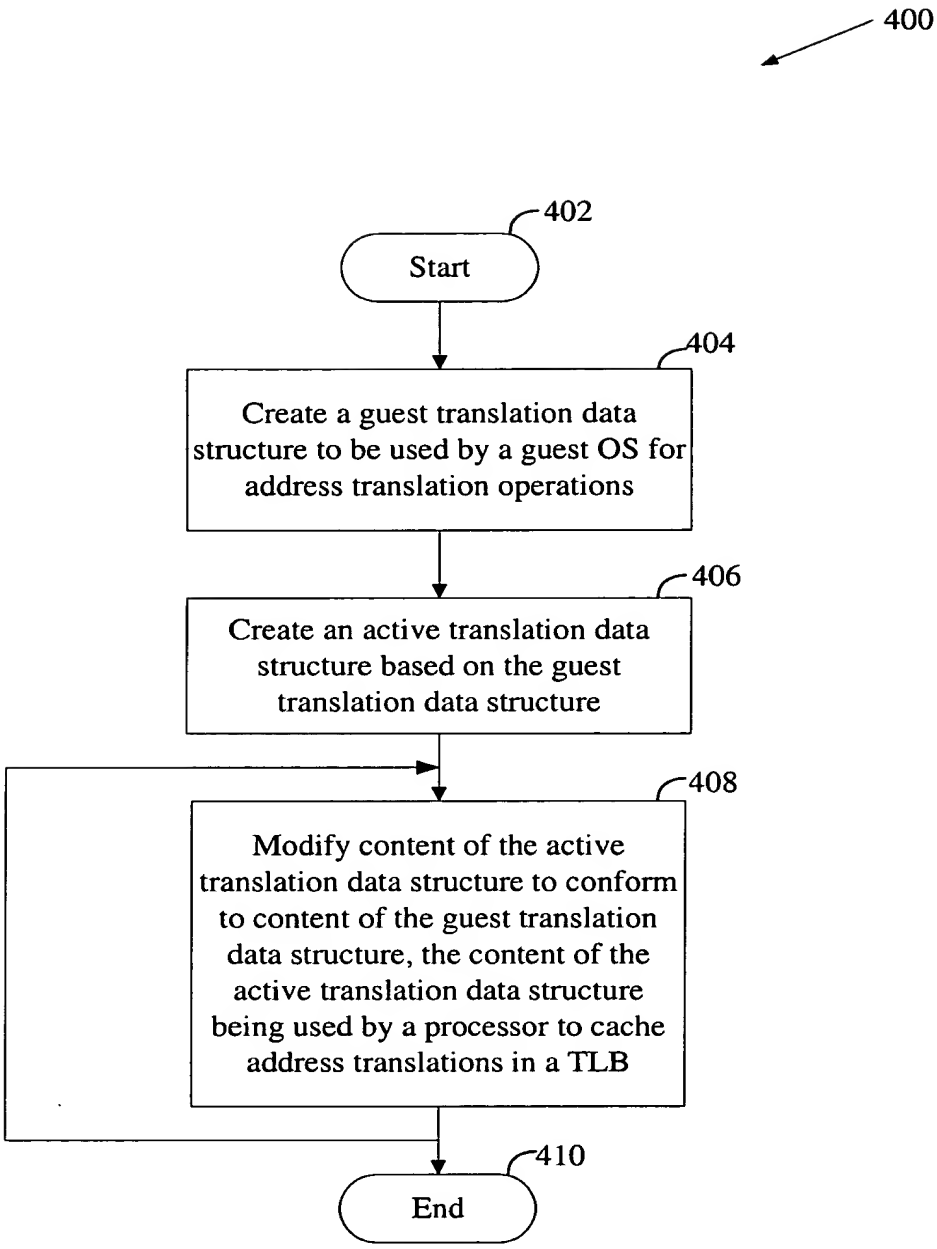


FIG. 4

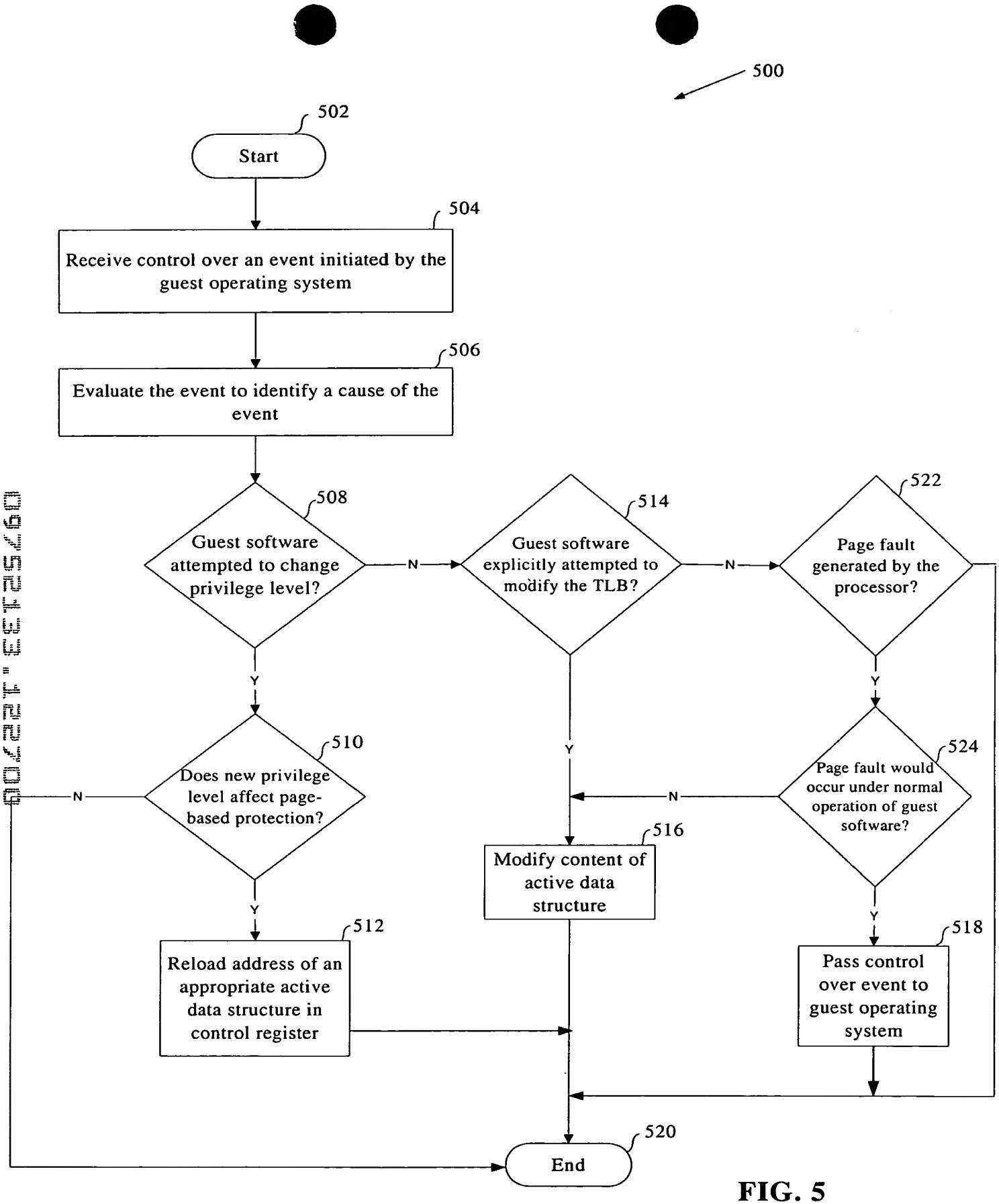

500
502
Start
504
Receive control over an event initiated by the guest operating system
506
Evaluate the event to identify a cause of the event
508
Guest software attempted to change privilege level?
N
514
Guest software explicitly attempted to modify the TLB?
N
522
Page fault generated by the processor?
Y
Y
Y
510
Does new privilege level affect page-based protection?
N
524
Page fault would occur under normal operation of guest software?
N
Y
Y
516
Modify content of active data structure
512
Reload address of an appropriate active data structure in control register
518
Pass control over event to guest operating system
520
End

FIG. 5

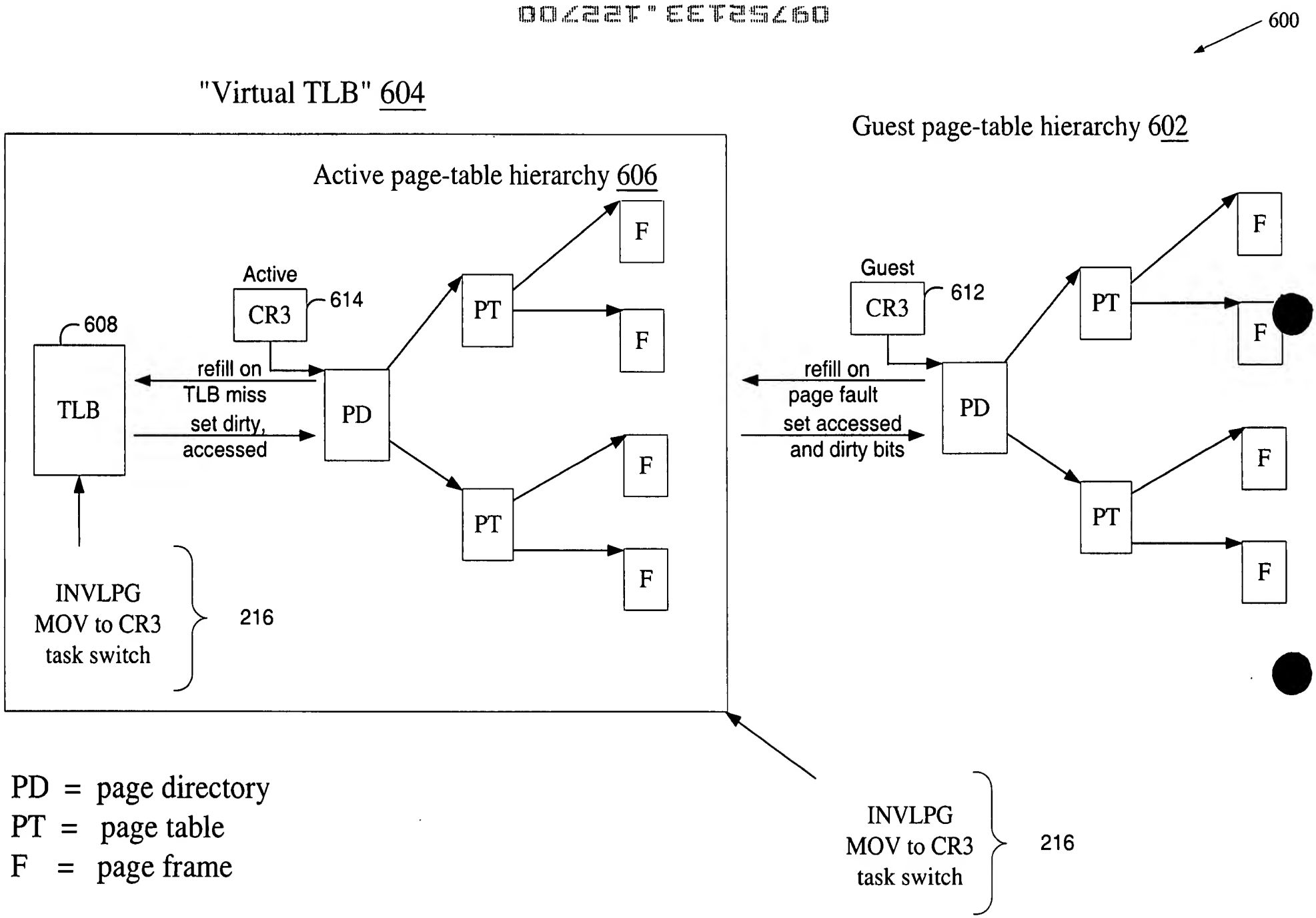

600
"Virtual TLB" 604
Active page-table hierarchy 606
Guest page-table hierarchy 602
608
TLB
Active
CR3
614
refill on
TLB miss
set dirty,
accessed
PD
PT
PT
F
F
F
F
INVLPG
MOV to CR3
task switch
216
Guest
CR3
612
refill on
page fault
set accessed
and dirty bits
PD
PT
PT
F
F
F
F
INVLPG
MOV to CR3
task switch
216
PD = page directory
PT = page table
F = page frame

FIG. 6

Document: US7,734,890

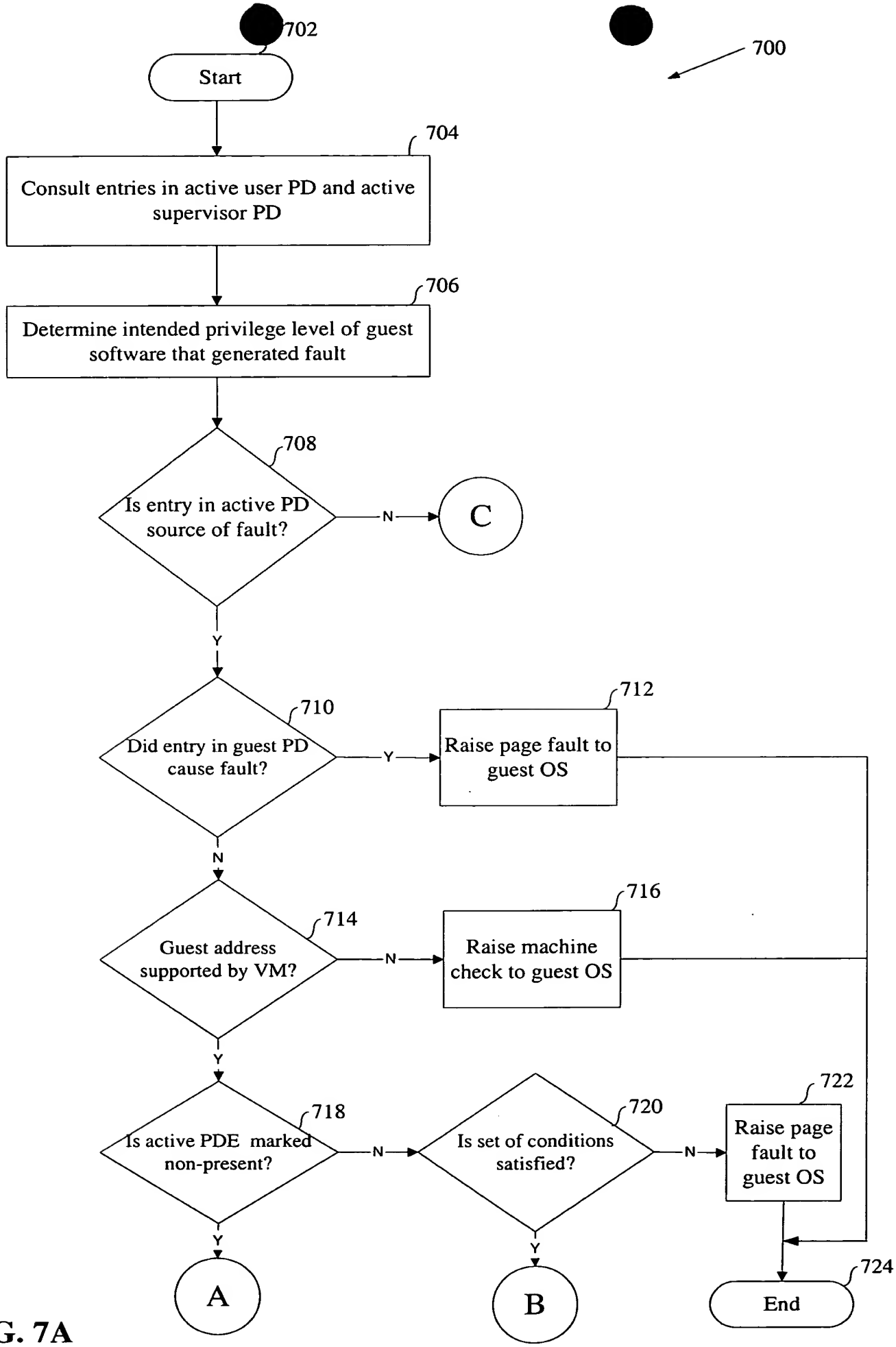


FIG. 7A

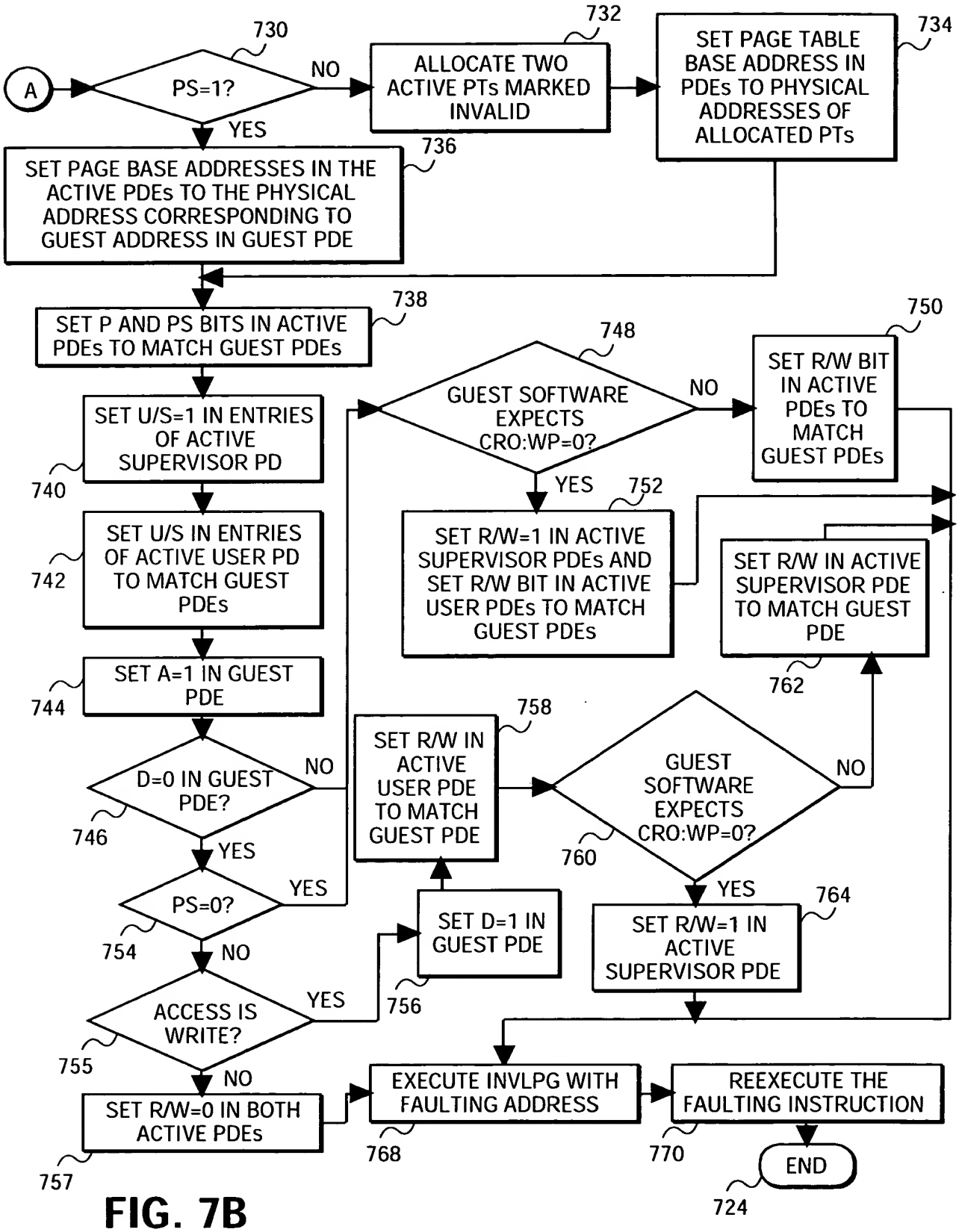

A
730
PS=1?
NO
YES
732
ALLOCATE TWO ACTIVE PTs MARKED INVALID
734
SET PAGE TABLE BASE ADDRESS IN PDEs TO PHYSICAL ADDRESSES OF ALLOCATED PTs
736
SET PAGE BASE ADDRESSES IN THE ACTIVE PDEs TO THE PHYSICAL ADDRESS CORRESPONDING TO GUEST ADDRESS IN GUEST PDE
738
SET P AND PS BITS IN ACTIVE PDEs TO MATCH GUEST PDEs
740
SET U/S=1 IN ENTRIES OF ACTIVE SUPERVISOR PD
742
SET U/S IN ENTRIES OF ACTIVE USER PD TO MATCH GUEST PDEs
744
SET A=1 IN GUEST PDE
746
D=0 IN GUEST PDE?
NO
YES
754
PS=0?
YES
NO
755
ACCESS IS WRITE?
YES
NO
757
SET R/W=0 IN BOTH ACTIVE PDEs
748
GUEST SOFTWARE EXPECTS CRO:WP=0?
NO
YES
750
SET R/W BIT IN ACTIVE PDEs TO MATCH GUEST PDEs
752
SET R/W=1 IN ACTIVE SUPERVISOR PDEs AND SET R/W BIT IN ACTIVE USER PDEs TO MATCH GUEST PDEs
762
SET R/W IN ACTIVE SUPERVISOR PDE TO MATCH GUEST PDE
758
SET R/W IN ACTIVE USER PDE TO MATCH GUEST PDE
760
GUEST SOFTWARE EXPECTS CRO:WP=0?
NO
YES
764
SET R/W=1 IN ACTIVE SUPERVISOR PDE
756
SET D=1 IN GUEST PDE
768
EXECUTE INVLPG WITH FAULTING ADDRESS
770
REEXECUTE THE FAULTING INSTRUCTION
724
END

FIG. 7B

DOCKET: 5030.P035

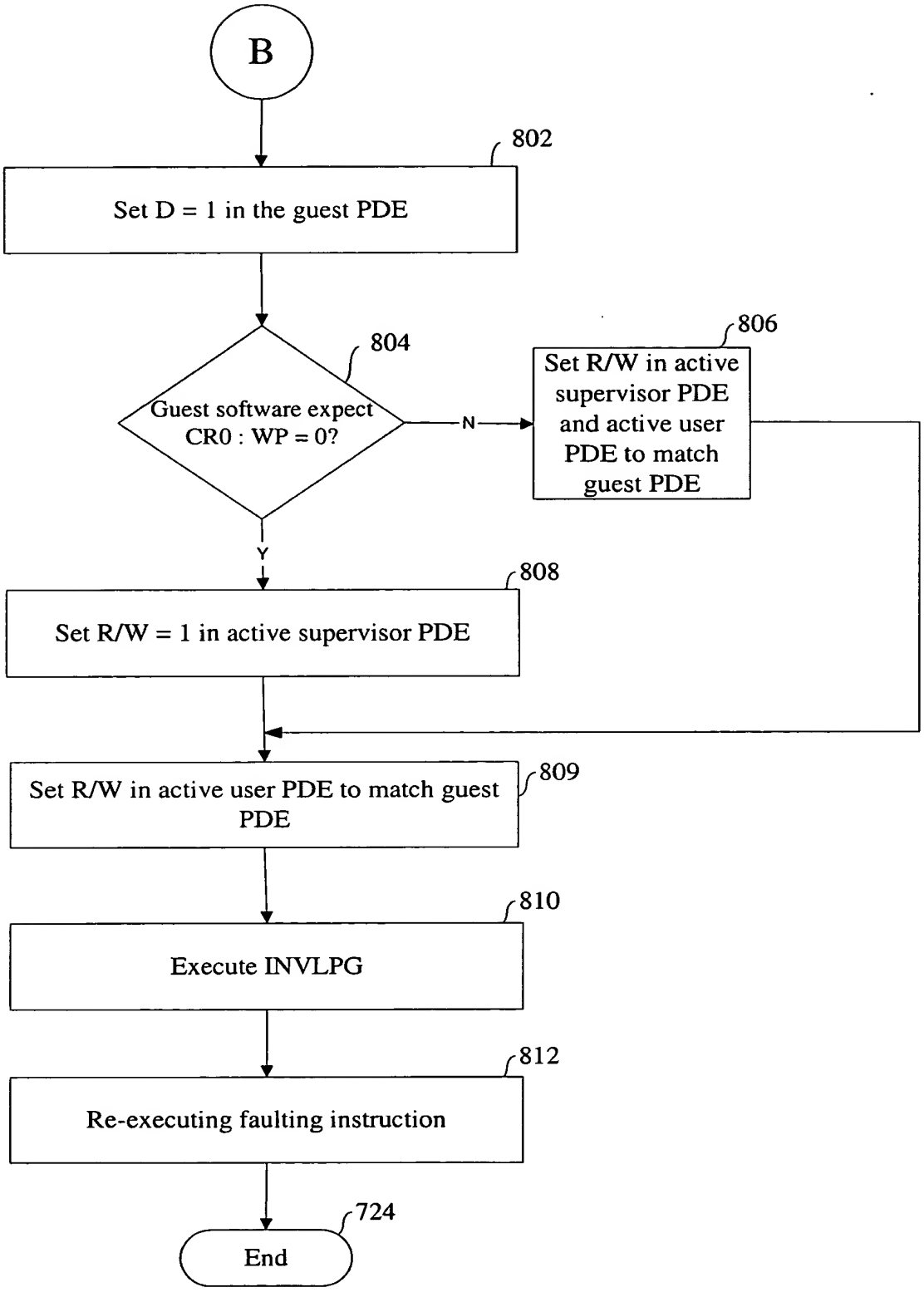


FIG. 7C

Docket No. 50325-1350

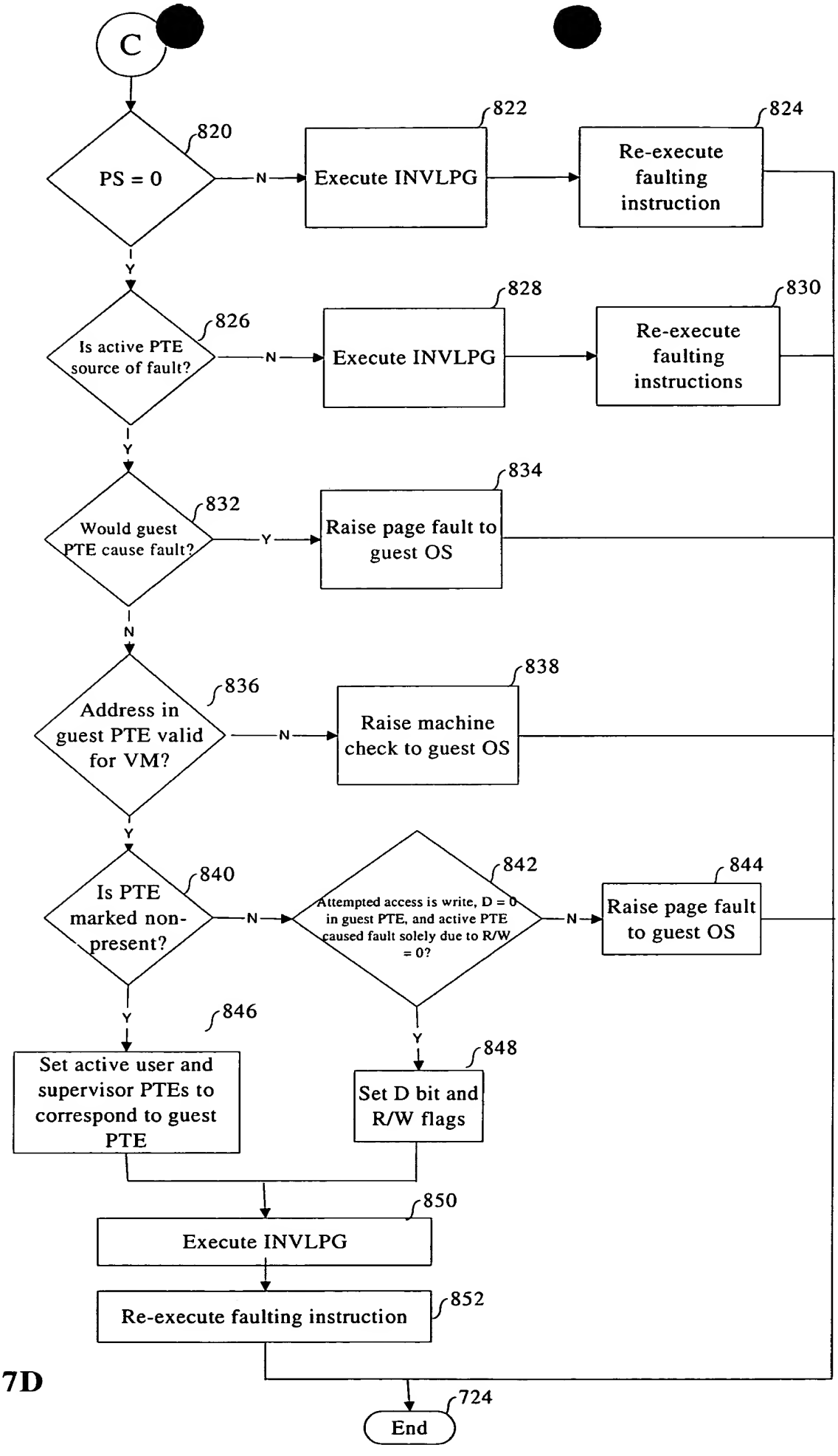


FIG. 7D

DOCKET: 5125.060

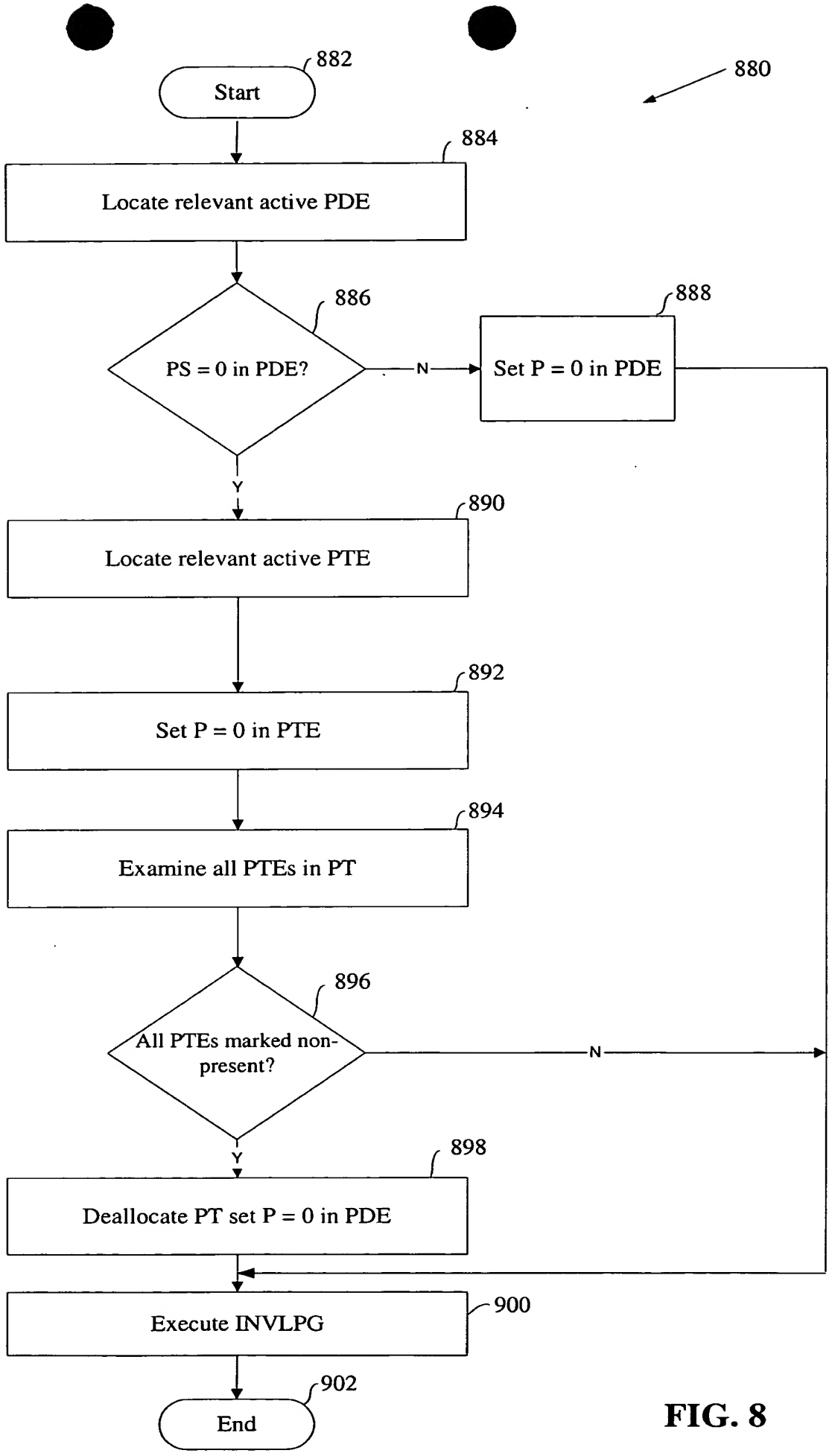


FIG. 8

0050-4150-0000

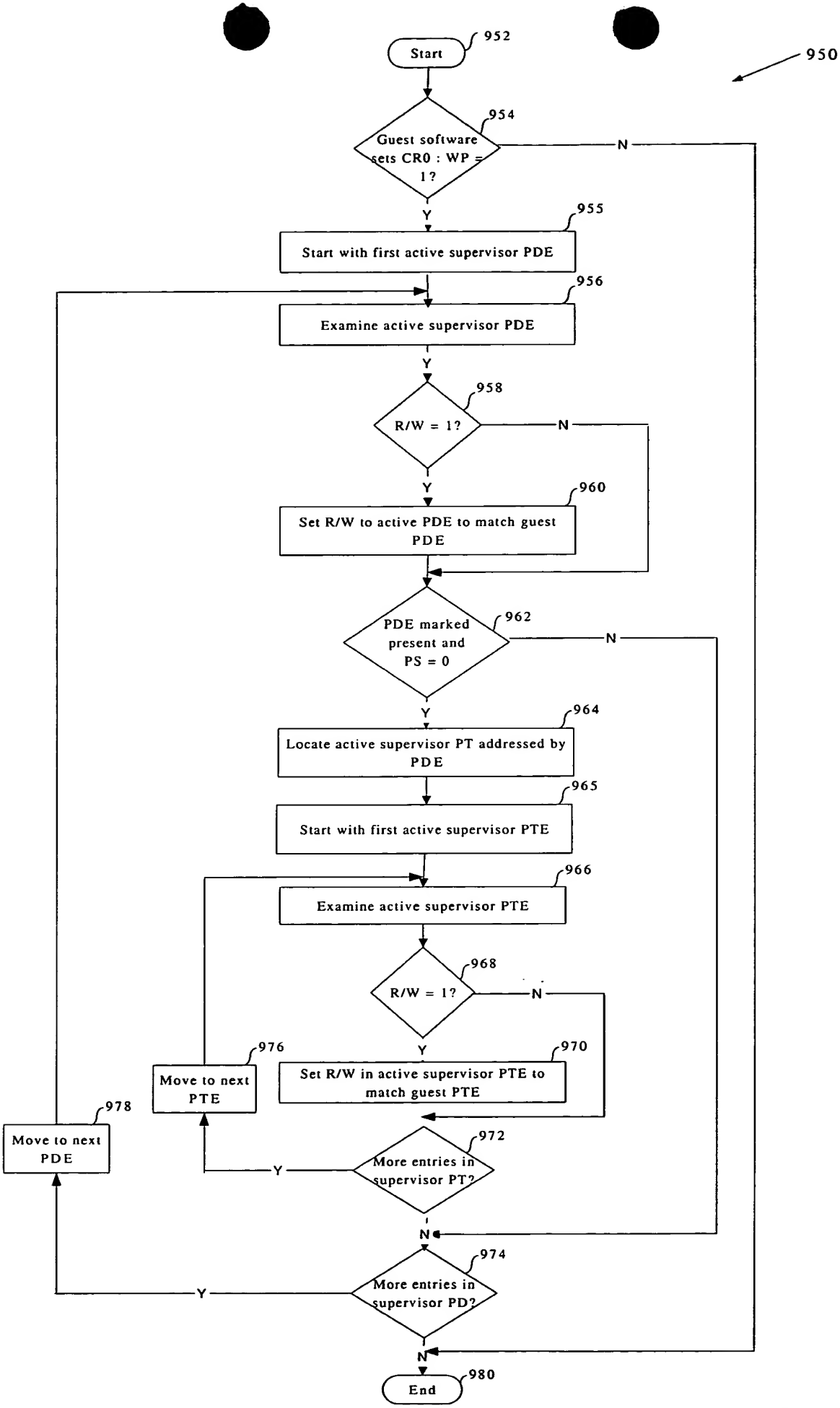


FIG. 9

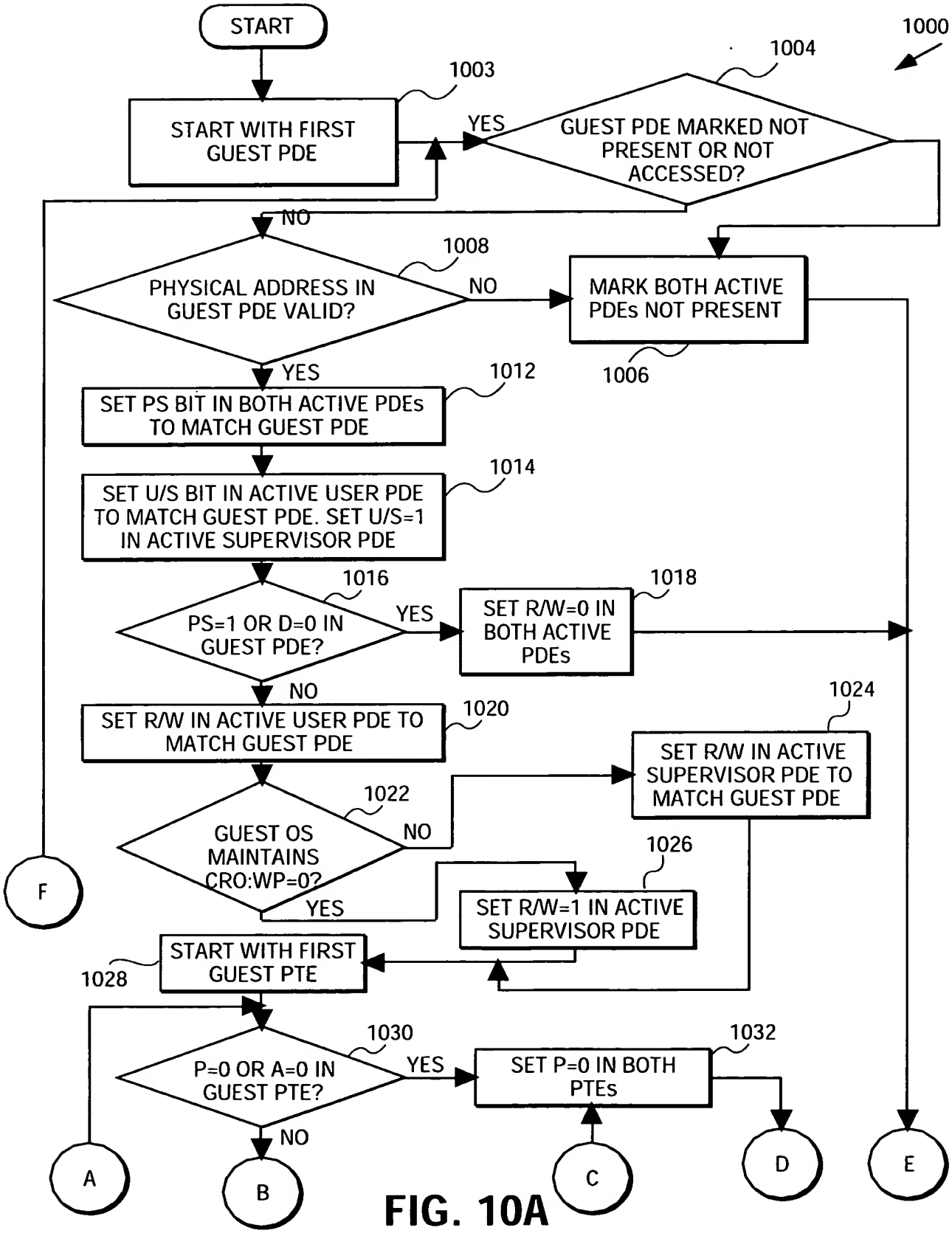

START
1000
1004
1003
START WITH FIRST GUEST PDE
YES
GUEST PDE MARKED NOT PRESENT OR NOT ACCESSED?
NO
1008
PHYSICAL ADDRESS IN GUEST PDE VALID?
NO
MARK BOTH ACTIVE PDEs NOT PRESENT
1006
YES
1012
SET PS BIT IN BOTH ACTIVE PDEs TO MATCH GUEST PDE
1014
SET U/S BIT IN ACTIVE USER PDE TO MATCH GUEST PDE. SET U/S=1 IN ACTIVE SUPERVISOR PDE
1016
PS=1 OR D=0 IN GUEST PDE?
YES
1018
SET R/W=0 IN BOTH ACTIVE PDEs
NO
1020
SET R/W IN ACTIVE USER PDE TO MATCH GUEST PDE
1024
SET R/W IN ACTIVE SUPERVISOR PDE TO MATCH GUEST PDE
1022
GUEST OS MAINTAINS CRO:WP=0?
NO
1026
YES
SET R/W=1 IN ACTIVE SUPERVISOR PDE
F
1028
START WITH FIRST GUEST PTE
1030
P=0 OR A=0 IN GUEST PTE?
YES
1032
SET P=0 IN BOTH PTEs
NO
A
B
C
D
E

FIG. 10A

DocketNo: 5150.0050

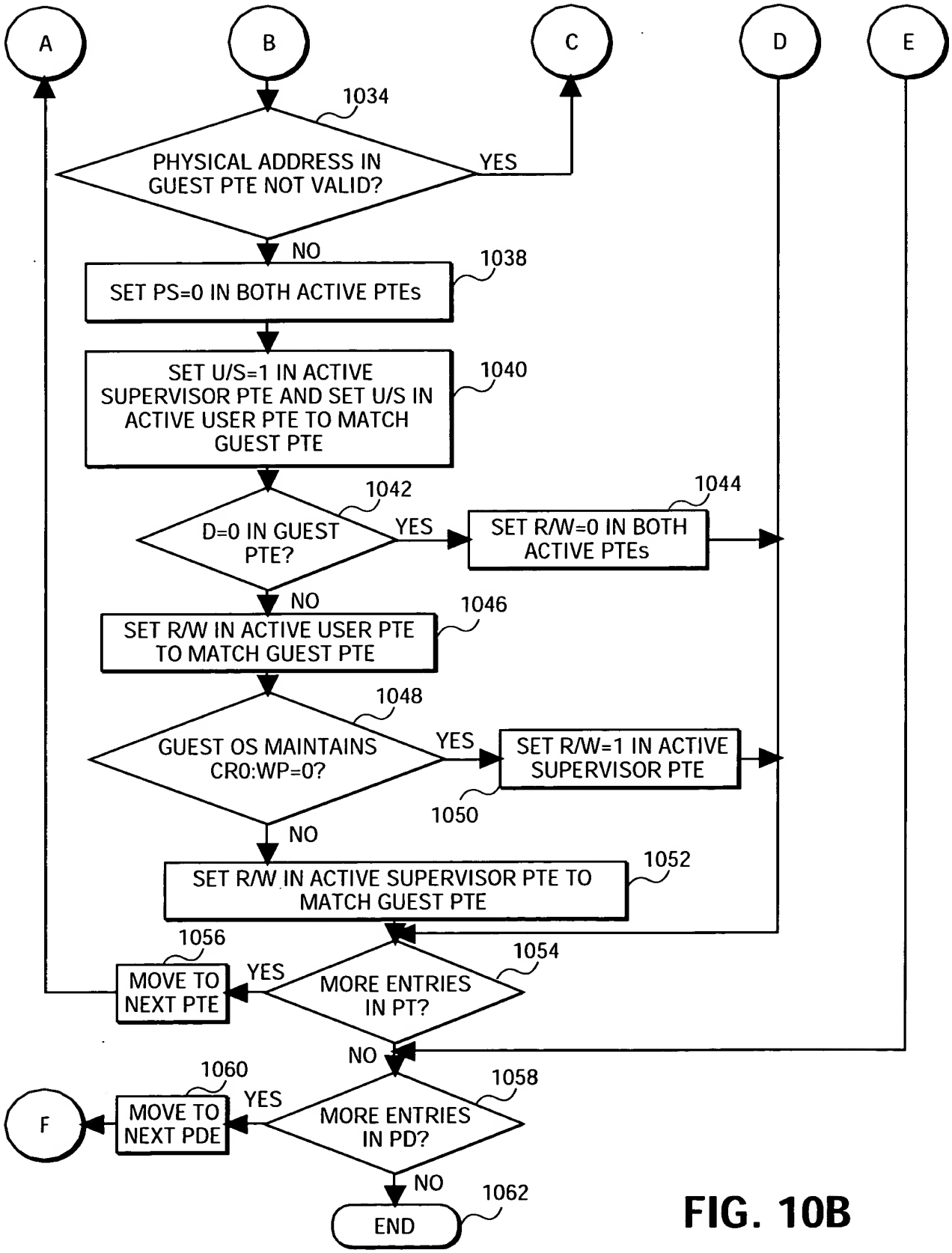


FIG. 10B

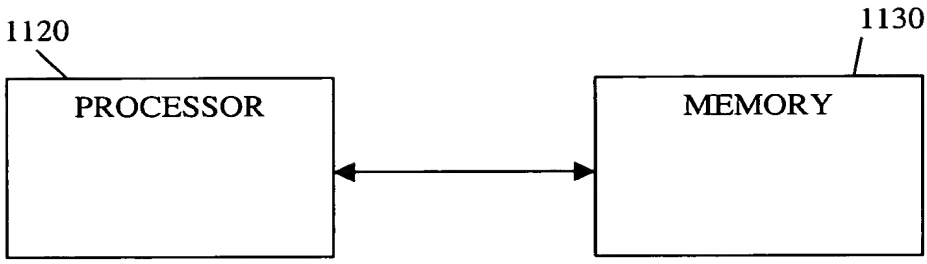


FIG. 11